Equational theories and the behavior of finite automata (Algebras, Languages, Algorithms and Computations)

Esik, Zoltan

数理解析研究所講究録
第 1769 巻 2011 年 122-123

Equational theories and the behavior of finite automata

Zoltán Ésik
Dept. of Computer Science
University of Szeged
Árpád tér 2
6720 Szeged, Hungary

May 25, 2011

The correctness of several constructions on automata only depends on some equational properties of the underlying structures. An axiomatic framework for finite automata is provided by the notions of Conway semirings and iteration semirings.

Conway semirings are semirings $S=(S,+,\cdot,0,1)$ equipped with a star operation $^*: S\rightarrow S$ satisfying the sum star and product star identities:

$$\begin{aligned}(a+b)^{*} &= (a^{*}b)^{*}a^{*}\\ (ab)^{*} &= 1+a(ba)^{*}b\end{aligned}$$

Iteration semirings also satisfy Conway's group identities associated with the finite groups. Sometimes the domain of definition of the star operation is restricted to a distinguished ideal giving rise to partial Conway and iteration semirings. Examples of iteration semirings include the semiring of all languages over an alphabet A, or just the semiring of regular languages over A. For any semiring S and alphabet A, the power series semiring $S\langle\langle A^{*}\rangle\rangle$ is a partial iteration semiring whose distinguished ideal is the collection of all proper series. And if S is itself an iteration semiring, then $S\langle\langle A^{*}\rangle\rangle$ is an iteration semiring. One can also form the (partial) iteration semirings of rational series.

The Conway semiring identities suffice to intoduce automata and automata behaviors and to establish a general Kleene theorem, and together with the group identities, they justify the validity of several other constructions such as minimization. In fact, the equational theory of regular languages can be axiomatized by the single equation $1^{*}=1$ relatively to iteration semirings, and there are several similar results known for rational power series.

Iteration semirings form a non-finitely based variety. However, in many applications the infinite collection of group identities may be replaced by a finite number of quasi-identities. Using this approach, several finite quasi-equational axiomatizations of the equational theory of regular languages and rational power series have been obtained.

Acknowledgement Partial support by grant no. K 75249 from the National Foundation of Hungary for Scientific Reseach (OTKA) and the TÁMOP-4.2.1/B-09/1/KONV-2010-0005 program "Creating the Center of Excellence at the University of Szeged", supported by the European Union and co-financed by the European Regional Fund, is acknowledged.